BEZPIECZEŃSTWO TEORIA I PRAKTYKA SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2022
No. 3 (XLVIII)

DOI: 10.48269/2451-0718-btip-2022-3-003
Received: 21.04.2022
Accepted: 22.05.2022

Robert Reczkowski

Col., PhD, Nicolaus Copernicus University in Toruń;
Doctrine and Training Centre of the Polish Armed Forces
https://orcid.org/0000-0001-7733-0815

Andrzej Lis

Col., PhD, Nicolaus Copernicus University in Toruń;
Doctrine and Training Centre of the Polish Armed Forces
https://orcid.org/0000-0003-4080-4137

Cognitive Warfare: what is our actual knowledge and how to build state resilience?

If you know the enemy and know yourself,
you need not fear the result of a hundred battles.
Sun Tzu

Introduction

The findings from the Polish Armed Forces project of strategic analysis NUP 2X35 indicate that "the contemporary security environment is becoming more and more volatile, uncertain, complex and ambiguous. At the same time, there is a deficit of understanding of the security environment, which results, among others, from the interpenetration of military and civilian aspects, the development of new technologies and globalisation processes and their multi-faceted consequences."[1] What is more, nowadays, the emergence of the new multipolar world order and increasing

[1] J. Mokrzycki, R. Reczkowski, S. Cieśla, Foreward, [in:] *Security Environment Out To 2035 – NUP 2X35: The Polish Perspective*, eds. *eidem*, Bydgoszcz: Doctrine and Training Centre of the Polish Armed Forces, 2020, p. 5.

competition among nations for their strategic positions in this new order are being observed. Besides traditional diplomatic and economic competition, this rivalry is more and more often conducted within the political and military dimensions of the security environment, where not only physical domains but also human cognition become an arena of rivalry.

According to the NATO official categorisation, there are five operational domains, i.e., land, sea, air, space, and cyberspace. For these officially recognised domains, strategic assumptions and operational concepts, as well as doctrines and tactical procedures have been developed. Nevertheless, none of these domains covers the battle space responsible for winning "hearts and minds." As noticed by Todd Schmidt, already "Chinese strategist and philosopher Sun Tzu[2] believed that wars are won through intelligence, information, and deception; attacking enemies where they are least prepared; and breaking resistance and subduing adversaries indirectly without fighting."[3] In consequence, cognitive studies and the cognitive domain of the operational environment become a focal point of contemporary warfare.

According to Lt. Gen. (Ret.) Vincent R. Stewart, former chief of the U.S. Defence Intelligence Agency, cognitive operations have become reality and will be the fifth-generation warfare.[4] Cognitive operations are of particular importance for countries, which conduct ideological penetration for strengthening morale and unity and for developing operational capabilities of their own forces, or for hampering morale, unity and operational capabilities of opposing parties. As confirmed by the studies conducted, among others, by Doctrine and Training Centre of the Polish Armed Forces, acquiring information and shaping decisional space before and during a conflict is a key success factor in contemporary conflicts. That is why it is predicted that in future war the struggle "for hearts and minds" may be won or lost without firing a single shot, even before a losing party realises that its interests are endangered – see the case of the Russian annexation of Crimea in 2014. Consequently, subject matter experts (SMEs) indicate that cognitive warfare is first and foremost focused on changing perception which triggers human behaviours. What is important, perception is an outcome of cognition, which makes a kind of a "mechanism" being a target for a potential aggressor.

---

2 Sun Tzu, *The Art of War*, CreateSpace Independent Publishing Platform, 12 November 2018.

3 T. Schmidt, "The Missing Domain of War: Achieving Cognitive Overmatch on Tomorrow's Battlefield", Modern War Institute, 4 July 2020, https://mwi.usma.edu/missing-domain-war-achieving-cognitive-overmatch-tomorrows-battlefield [accessed: 13 January 2022].

4 K. Underwood, "Cognitive Warfare Will Be Deciding Factor in Battle", *SIGNAL*, 15 August 2017, https://www.afcea.org/content/cognitive-warfare-will-be-deciding-factor-battle [accessed: 19 December 2021]; "For the Greater Good: Reflections on Legacy with Vincent Stewart", DIA Public Affairs, 24 February 2022, https://www.dia.mil/News-Features/Articles/Article-View/Article/2945317/for-the-greater-good-reflections-on-legacy-with-vincent-stewart [accessed: 27 February 2022].

The aim of the paper is to identify and explore the key assumptions of cognitive warfare. The research process is focused on the following study questions: (1) What are the characteristics of cognitive warfare? (2) How can cognitive operations build an advantage over a competitor? (3) How to build resilience to cognitive operations?

The analysis is based on the data collected with the use of the method of narrative literature review. The authors are aware of the limitations resulting from the methodological shortcomings of this method.[5] Nevertheless, due to a very limited number of sources, a systematic literature review[6] was not possible. The search for publications indexed in the Scopus database and including the phrase "cognitive warfare" in their titles, conducted as of 19 April 2022, resulted in finding only one publication.[7] Extending the scope of the search to titles, keywords, and abstracts brought about one more item; however, irrelevant for the purpose of the study. Thus, narrative literature review, which is considered to be very relevant for studying scant and emerging research fields, was chosen as a method of collecting data for analysis. Moreover, the authors' participatory observations and lessons from national and international military research projects contributed to understanding and discussing the gist of cognitive warfare.

Results

Defining cognitive warfare

The outcomes of cognitive studies indicate numerous attempts to define cognitive warfare both in the civilian academia and in the military. Nevertheless, there is still no commonly accepted definition which could become the foundation of doctrinal assumptions or procedures for the entities of the national security system.

---

5 D. Tranfield, D. Denyer, P. Smart, "Towards a Methodology for Developing Evidence-informed Management Knowledge by Means of Systematic Review", *British Journal of Management*, vol. 14, issue 3, 2003, pp. 207–222, https://doi.org/10.1111/1467-8551.00375; W. Czakon, "Metodyka systematycznego przeglądu literatury", *Przegląd Organizacji*, no. 3, 2011, pp. 57–61, https://doi.org/10.33141/po.2011.03.13.

6 D.J. Cook, C.D. Mulrow, R.B. Haynes, "Systematic Reviews: Synthesis of Best Evidence for Clinical Decisions", *Annals of Internal Medicine*, vol. 126, issue 5, 1997, pp. 376–380, https://doi.org/10.7326/0003-4819-126-5-199703010-00006; A. Booth, D. Papaioannou, A. Sutton, *Systematic Approaches to a Successful Literature Review*, London: SAGE Publications Ltd, 2012; Z. Mazur, A. Orłowska, "Jak zaplanować i przeprowadzić systematyczny przegląd literatury", *Polskie Forum Psychologiczne*, vol. 23, no. 2, 2018, pp. 235–251, https://doi.org/10.14656/PFP20180202.

7 R.A. Landes, Orientalism as Caliphator Cognitive Warfare: Consequences of Edward Saïd's Defense of the Orient, [in:] *Handbook of Research on Contemporary Approaches to Orientalism in Media and Beyond*, vol. 1, eds. I. Tombul, G. Sari, Hershey, PA: IGI Global, 2021, pp. 33–52, https://doi.org/10.4018/978-1-7998-7180-4ch003.

In order to understand cognitive warfare, it is first necessary to define the term "cognition" which is associated with human mind. Human brain operates all the time as it incessantly absorbs, transforms, plans, orders and remembers data, information, and knowledge. As noticed by an established cognitive researcher Daniel Kahneman, in a day-to-day routine, this activity is not recognised. This is only one aspect of complex cognitive processes. Cognition is thinking, which encompasses processes connected with perception, knowledge, problem solving, assessment, language, and memory. Cognitive researchers try to understand the way in which humans integrate, organise, and use conscious cognitive experiences without recognising subconscious operations of the brain.[8] Thus, the area where cognitive warfare is conducted (in some documents defined as a "cognitive domain") consists of "perception and reasoning in which manoeuvre is achieved by exploiting the information environment to influence interconnected beliefs, values, and culture of individuals, groups, and/or populations."[9]

The aforementioned characteristics of cognition and a cognitive domain constitute the foundation for defining cognitive warfare. For instance, Richard A. Landes describes cognitive warfare as "warfare undertaken by the weak side in an asymmetrical conflict, manipulation of information and ideas designed to convince the stronger side not to use its superior strength, to make patriots of one's own and pacifists of the enemy, to redeploy in order to better fight the kinetic (military) war."[10] In a similar way, Zac Rogers points out that "cognitive warfare is not only an attack on what we think. It is an attack on our way of thinking."[11] Paul Ottewell defines cognitive warfare as "manoeuvres in the cognitive domain to establish a predetermined perception among a target audience in order to gain advantage over another party."[12] In turn, Oliver Backes and Andrew Swab understand cognitive warfare as "a strategy that focuses on altering [through information means,] how a target population thinks – and through that how it acts."[13] Analysing the context of the Russian influence on elections in the Baltic states, they indicate that the main aim of cognitive warfare is "[...] to undermine or shape domestic political processes by changing mindsets," and that "cognitive warfare weaponizes information

---

8 D. Kahneman, *Thinking, Fast and Slow*, New York: Farrar, Straus, and Giroux, [cop. 2011], pp. 18–20.

9 P. Ottewell, "Defining the Cognitive Domain", *Over The Horizon*, 7 December 2020, https://othjournal.com/2020/12/07/defining-the-cognitive-domain [accessed: 11 January 2022].

10 R.A. Landes, *op. cit.*, p. 51.

11 Z. Rogers, "In the Cognitive War – The Weapon is You!", The Mad Scientist Laboratory blog, 1 July 2019, https://madsciblog.tradoc.army.mil/158-in-the-cognitive-war-the-weapon-is-you [accessed: 27 December 2021].

12 P. Ottewell, *op. cit*.

13 O. Backes, A. Swab, *Cognitive Warfare. The Russian Threat to Election Integrity in the Baltic States*, Cambridge: Belfer Center for Science and International Affairs, 2019, p. 8.

to persuade or confuse populations and shift public opinion, often tapping into real divisions in Baltic societies to drive wedges between the state and potentially sympathetic populations."[14]

The aforementioned definitions and opinions point out that the objective of cognitive warfare is to influence and/or destabilise a competitor through a change in human thinking and behaviours. However, it is highlighted that the ultimate aim is to achieve some advantage (e.g. mental, psychological, or informational advantage) over another party. Summing up, the aim of cognitive warfare is to achieve a change in behaviours of the target audience through a cognitive process favourable to an attacking state (or a non-state actor). Therefore, as rightly observed by a Norwegian researcher Lea Kristina Bjørgul, the aim of cognitive warfare is the same as in other types of warfare, i.e., to impose the will on the other state. As stated by Bjørgul "this is in line with one of the main elements of Clausewitz's definition of war: '…an act of violence intended to compel our opponent to fulfill our will' […]. According to Clausewitz, war is conducted for some second-order purpose. States do not go to war simply to commit violence, but to impose their will upon other states."[15]

Gaining advantage through cognitive warfare

As noticed by military experts, in spite of some similarities, there are significant differences between operations in a cognitive domain and other physical operational domains, such as land, sea, air, and space. Firstly, cognitive warfare is non-kinetic warfare. Thus, in a cognitive domain it is possible to win without using conventional power. Such an effect may be achieved, e.g., by informational influence on a potential adversary changing perception before the opposing party realises that its interests are endangered. Moreover, it is worth mentioning that cases of changes in human perception resulting from the use of micro-wave weapons, which cause damages to the brain and hamper cognitive processes, have already been noted.[16]

Therefore, it should be highlighted that human minds become the battlefield in cognitive warfare and the consequence of this struggle is a change in what humans think and how they think and act. This struggle is taken up in order to shape and influence individual and team beliefs and behaviours, and consequently, contribute to achieving strategic, operational, or tactical aims and objectives of an aggressor. In its extreme form, cognitive warfare shows potential to polarise and divide the whole society, resulting in hampering or even destroying collective will of the society to resist

---

[14] *Ibidem*.

[15] L.K. Bjørgul, "Cognitive Warfare and the Use of Force", *Stratagem*, 3 November 2021, https://www.stratagem.no/cognitive-warfare-and-the-use-of-force [accessed: 15 December 2021].

[16] S.L. Myers, J. Perlez, "U.S. Diplomats Evacuated in China as Medical Mystery Grows", *New York Times*, 6 June 2018, https://www.nytimes.com/2018/06/06/world/asia/china-guangzhou-consulate-sonic-attack.html [accessed: 12 February 2022].

the aggressor's intention. In such a case, an attacking party may take control over the society without using force or coercion.

The objectives of cognitive warfare may be both limited to short periods of time and long-term and strategic with campaigns conducted for several years or even decades. A single campaign may be concentrated on a particular objective, e.g., preventing the conduct of a strategic manoeuvre in accordance with a plan or enforcing a change in social behaviours. Other campaigns may be conducted in order to disrupt the functioning of societies or allies in the long-term perspective, e.g., by sowing doubts about legitimacy and effectiveness of governments, hampering democratic processes, triggering social unrest, or inciting separatist movements.

As observed by researchers from John Hopkins University and Imperial College London conducting their studies under the supervision of Lawrence Aronhime and Alexander Cocron, "today, cognitive warfare integrates cyber, information, psychological, and social engineering capabilities to achieve its ends. It takes advantage of the internet and social media to target influential individuals, specific groups, and large numbers of citizens selectively and serially in a society. It seeks to sow doubt, to introduce conflicting narratives, to polarise opinion, to radicalise groups, and to motivate them to acts that can disrupt or fragment an otherwise cohesive society. And the widespread use of social media and smart device technologies in Alliance member countries may make them particularly vulnerable to this kind of attack."[17]

How to build resilience?

Cognitive warfare may influence any aspect of the functioning of societies. What is more, operations in the cognitive domain are usually associated with long-lasting, unlimited war in the "grey zone" (i.e., below the threshold of an armed conflict). In this context, such operations attack the social capital of a nation, which results in questioning defensive actions and influences attitudes and reactions to the aggressor's provocations. It should be highlighted that cognitive warfare cannot be limited to information operations, social engineering, or a struggle for "hearts and minds," but it should be extended to all areas of activity of individuals and societies, where ideological attacks are possible.

In order to build state resilience, it should first and foremost be taken into account that nowadays cognitive operations are of particular interest to some non-democratic states which may use them as an element of rivalry against Western societies. Their operations will usually be conducted below the threshold of NATO's Article 5 and below the violence level necessary to convince the United Nations Security Council

[17] K. Cao, S. Glaister, A. Pena, D. Rhee, W. Rong, A. Rovalino, S. Bishop, R. Khanna, J.S. Saini, "Countering Cognitive Warfare: Awareness and Resilience", *NATO Review*, 20 May 2021, https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html [accessed: 16 December 2021].

to enact the resolution (unless new "red lines" for those countries are drawn, crossing of which will result in an open conflict). Consequently, in the contemporary era of rivalry of powers, cognitive operations will be permanently employed by these powers (and also by some other nations) to achieve their own objectives. Thus, Poland may expect some challenges and threats to its security, originating from cognitive warfare operations of potential competitors. In order to mitigate the effects of these challenges and threats, and to increase a state's resilience in the cognitive domain, the following actions are worth considering:

- conducting analytical studies in order to develop situational (operational) awareness, recognise risks and their consequences for the national security, as well as to be able to differentiate facts from opinions, the truth from falsity, and evidence from presumptions;
- changing perception of threats to the state security because numerous threats will originate from adversary's actions below the threshold of an open armed conflict ("grey zone") and will be connected with its influence on society;
- increasing effectiveness of strategic communications (StratCom) through combining all activities of Public Diplomacy, Public Affairs, InfoOps, and PsyOps, and coordinating them at the political-strategic level;
- making efforts to understand the desired end state of adversary's operation in the context of ambiguity of conflicts in the "grey zone";
- impeding cognitive warfare of an adversary to prevent achieving the expected reaction of the target audience;
- avoiding mistakes in setting the limits of accepted risks ("red lines") for a potential competitor;
- conducting continuous assessment of own susceptibility in all dimensions of PMESII, as well as assessing advancement and advantages of a potential competitor in these dimensions;
- employing new technologies (e.g., AI, Big Data) in order to gain advantage in cognitive operations, including capability to counteract this type of attacks.

Discussion and Conclusions

As noticed by Marie-Pierre Raymond from Defence Research and Development Canada (DRDC), the processes of digitalisation have opened new opportunities for a potential adversary to conduct operations in the "grey zone," below the threshold of an armed conflict. Cognitive operations employing "social media, social networking, social messaging, and mobile device technologies" show high potential to influence "information, beliefs, values, and cultures." Thus, narrative wars, which focus on manipulating and controlling human reactions to information, in

some circumstances may replace conventional wars.[18] Cognitive warfare may be conducted with the use of a variety of methods and means. Nowadays, a widespread use of social media platforms enables state and non-state rivals to attack individuals, selected groups, or even whole societies through messaging, influencing social media, selective sharing of documents and video files, etc. Moreover, cyber operations capabilities enable them to hack and track individuals or social networks. Analyses point out that advantage in cognitive warfare, at least in the first stage of confrontation, will be most likely achieved by the first mover, i.e., a party choosing the time, location, and means of cognitive operations.

Taking into account the use of the aforementioned methods and means, building resilience to cognitive warfare starts with understanding its gist and recognising its characteristics. Next steps include discovering when a cognitive campaign is conducted as well as identifying its origins, aims, and the parties engaged.[19] Nevertheless, it is necessary to be aware that:

- cognitive operations are usually covert operations, which closely relate to the so-called war of ideology, but they are rarely connected with a direct confrontation or kinetic actions;
- failure in counteracting cognitive warfare attacks and building sustainable and proactive capability to act in a cognitive domain may result in inevitability of engaging in a kinetic conflict;
- kinetic capabilities may be a decisive factor in rivalry; however, long-term outcomes are greatly dependent on the capability to influence the cognitive domain.

Summing up, the study has identified and explored the key assumptions of cognitive warfare. In response to the first study question concerning the characteristics of cognitive warfare and having analysed a variety of definitions and opinions, we assume that the objective of cognitive warfare is to influence and/or destabilise a competitor through a change in human thinking and behaviours in order to achieve advantage (including mental, psychological or informational advantage) over another party. In response to the second study question, we realise that cognitive operations build an advantage over a competitor by changing what humans think and how they think and act, shaping and influencing individual and team beliefs and behaviours, and consequently, contributing to achieving strategic, operational, or tactical aims and objectives of an attacking party. Cognitive warfare integrates a variety of means including cyber, information, psychological, and social engineering capabilities. Cognitive operations may be targeted at individuals, specific groups, and whole societies. They range from short-term tactical operations

[18] Government of Canada, "Defending Canada Against Cognitive Warfare", 22 November 2021, https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2021/11/defending-canada-cognitive-warfare.html [accessed: 11 January 2022].

[19] K. Cao, S. Glaister, A. Pena, D. Rhee, W. Rong, A. Rovalino, S. Bishop, R. Khanna, J.S. Saini, *op. cit.*

to long-term strategic campaigns. In response to the third study question, we identify a catalogue of recommended actions aimed at building and strengthening resilience to cognitive operations. They include conducting analytical studies in order to develop situational awareness, changing perception of threats to state security, increasing effectiveness of strategic communications (StratCom), recognising real end state of an adversary's operations, developing capabilities to impede potential cognitive operations of an adversary, analysing own vulnerabilities on a continuous basis, and employing emerging and disruptive technologies to strengthen own capabilities.

When discussing the findings of the study, its methodological limitations should be taken into account. Firstly, due to the theoretical character of the article, the method of literature review was the means to achieve the aim of the study. Nevertheless, there was no triangulation with any other method of study, which should be considered as a weakness of the adopted methodology. Secondly, as already mentioned, cognitive warfare is still an emerging stream of research, and very scant literature is available. Consequently, the employment of a systematic literature review as a method of study was not possible and the method of narrative literature review, showing a lower level of scientific rigor, was used.

Taking into account the findings of our analysis, cognitive warfare seems to be an interesting and emerging research stream in security studies. Therefore, some lines of further research are worth mentioning. Firstly, a growing number of theoretical publications discussing the assumptions and characteristics of cognitive warfare and cognitive operations lays foundations for studies employing heuristic methods (known in NATO as alternative analysis or ALTA methods) in order to identify and categorise manifestations of cognitive operations, their techniques and instruments as well as relationships with operations conducted in other operational domains. Secondly, developing possible models of an escalation ladder or an escalation matrix in the cognitive domain and later testing them, e.g., with the use of wargaming methodology, open new opportunities for operationalising the cognitive domain. Thirdly, analysing case studies and lessons from the conduct of cognitive operations in military exercises and their employment in real-life competition below the threshold of an armed conflict constitutes the next recommended line of prospective research on cognitive warfare.

References

Backes O., Swab A., *Cognitive Warfare. The Russian Threat to Election Integrity in the Baltic States*, Cambridge: Belfer Center for Science and International Affairs, 2019.

Bjørgul L.K., "Cognitive Warfare and the Use of Force", Stratagem, 3 November 2021, https://www.stratagem.no/cognitive-warfare-and-the-use-of-force [accessed: 15 December 2021].

Booth A., Papaioannou D., Sutton A., *Systematic Approaches to a Successful Literature Review*, London: SAGE Publications Ltd, 2012.

Cao K., Glaister S., Pena A., Rhee D., Rong W., Rovalino A., Bishop S., Khanna R., Saini J.S., "Countering Cognitive Warfare: Awareness and Resilience", *NATO Review*, 20 May 2021, https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html [accessed: 16 December 2021].

Cook D.J., Mulrow C.D., Haynes R.B., "Systematic Reviews: Synthesis of Best Evidence for Clinical Decisions", *Annals of Internal Medicine*, vol. 126, issue 5, 1997, pp. 376–380, https://doi.org/10.7326/0003-4819-126-5-199703010-00006.

Czakon W., "Metodyka systematycznego przeglądu literatury", *Przegląd Organizacji*, no. 3, 2011, pp. 57–61, https://doi.org/10.33141/po.2011.03.13.

"For the Greater Good: Reflections on Legacy with Vincent Stewart", DIA Public Affairs, 24 February 2022, https://www.dia.mil/News-Features/Articles/Article-View/Article/2945317/for-the-greater-good-reflections-on-legacy-with-vincent-stewart/ [accessed: 27 February 2022].

Government of Canada "Defending Canada Against Cognitive Warfare", 22 November 2021, https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2021/11/defending-canada-cognitive-warfare.html [accessed: 11 January 2022].

Kahneman D., *Thinking, Fast and Slow*, New York: Farrar, Straus, and Giroux, [cop. 2011].

Landes R.A., Orientalism as Caliphator Cognitive Warfare: Consequences of Edward Saïd's Defense of the Orient, [in:] *Handbook of Research on Contemporary Approaches to Orientalism in Media and Beyond*, vol. 1, eds. I. Tombul, G. Sari, Hershey, PA: IGI Global, 2021, pp. 33–52, https://doi.org/10.4018/978-1-7998-7180-4ch003.

Mazur Z., Orłowska A., "Jak zaplanować i przeprowadzić systematyczny przegląd literatury", *Polskie Forum Psychologiczne*, vol. 23, no. 2, 2018, pp. 235–251, https://doi.org/10.14656/PFP20180202.

Mokrzycki J., Reczkowski R., Cieśla S., Foreward, [in:] *Security Environment Out To 2035 – NUP 2X35: The Polish Perspective*, eds. J. Mokrzycki, R. Reczkowski, S. Cieśla, Bydgoszcz: Doctrine and Training Centre of the Polish Armed Forces, 2020, pp. 5–6.

Myers S.L., Perlez J., "U.S. Diplomats Evacuated in China as Medical Mystery Grows", *New York Times*, 6 June 2018, https://www.nytimes.com/2018/06/06/world/asia/china-guangzhou-consulate-sonic-attack.html [accessed: 12 February 2022].

Ottewell P., "Defining the Cognitive Domain", *Over the Horizon*, 7 December 2020, https://othjournal.com/2020/12/07/defining-the-cognitive-domain [accessed: 11 January 2022].

Rogers Z., "In the Cognitive War – The Weapon is You!", The Mad Scientist Laboratory blog, 1 July 2019, https://madsciblog.tradoc.army.mil/158-in-the-cognitive-war-the-weapon-is-you [accessed: 27 December 2021].

Schmidt T., "The Missing Domain of War: Achieving Cognitive Overmatch on Tomorrow's Battlefield", Modern War Institute, 4 July 2020, https://mwi.usma.edu/missing-domain-war-achieving-cognitive-overmatch-tomorrows-battlefield [accessed: 13 January 2022].

Sun Tzu, *The Art of War*, CreateSpace Independent Publishing Platform, 12 November 2018.

Tranfield D., Denyer D., Smart P., "Towards a Methodology for Developing Evidence-informed Management Knowledge by Means of Systematic Review", *British Journal of Management*, vol. 14, issue 3, 2003, pp. 207–222, https://doi.org/10.1111/1467-8551.00375.

Underwood K., "Cognitive Warfare Will Be Deciding Factor in Battle", *SIGNAL*, 15 August 2017, https://www.afcea.org/content/cognitive-warfare-will-be-deciding-factor-battle [accessed: 19 December 2021].

Cognitive Warfare: what is our actual knowledge and how to build state resilience?

Abstract

Contemporary national security systems face many challenges related to the changes taking place in the security and operating environments. Cognitive warfare, listed as one of such challenges, is often described as "the struggle for hearts and minds" because in cognitive warfare it is the human mind that becomes the battlefield. The aim of the paper is to identify and explore the key assumptions of cognitive warfare. The research process is focused on the following study questions: (1) What are the characteristics of cognitive warfare? (2) How can cognitive operations build an advantage over a competitor? (3) How to build resilience to cognitive operations? The analysis is based on the data collected with the use of the method of narrative literature review. Moreover, the authors' participatory observations and lessons from national and international military research projects contributed to understanding and discussing the gist of cognitive warfare.

Key words: cognitive warfare, cognitive domain, security environment, awareness, resilience